7M

УДК 681.3; 004.056.53

Е.П. Максимович, А.Б. Степанян, В.К. Фисенко
Объединенный институт проблем информатики НАН Беларуси, г. Минск
Беларусь, 220012, г. Минск, ул. Сурганова, 6

Методологические основы поддержки принятия решения при анализе информационной безопасности в процессе эксплуатации информационных систем

E.P. Maksimovich, A.B. Stepanyan, V.K. Fisenko
United Institute of Informatics Problems of the National Academy of Sciences of Belarus, c. Minsk, Belarus
Belarus, 220012, , c. Minsk, Surganova st., 6

Methodological Foundations to Support Decision-Making in the Analysis of Information Security During the Information System Operation

О.П. Максимович, А.Б. Степанян, В.К. Фісенко
Об’єднаний інститут проблем інформатики НАН Білорусі, м. Мінськ
Білорусь, 220012, м. Мінськ, вул. Сурганова, 6

Методологічні основи підтримки прийняття рішення при аналізі інформаційної безпеки в процесі експлуатації інформаційних систем

Статья посвящена проблеме оценки защищенности информационной систем в реальных условиях эксплуатации, являющейся одной из ключевых задач поддержки требуемого уровня информационной безопасности в процессе жизненного цикла системы. Предлагается подход к построению системы поддержки принятия решения, позволяющий за счет автоматизации процесса оценки и использования накопленного экспертного опыта одновременно повысить качество оценки и уменьшить трудоемкость процесса оценки.
Ключевые слова: информационная безопасность, система защиты информации, система поддержки принятия решения

The paper deals with the problem of information systems security estimation in real-world conditions, as one of the key tasks of supporting the required level of information security through the life cycle of the system. Proposed approach to the construction of the decision support system allows to automate the estimation process on the base of the expertise and to improve quality of the estimation and reduce costs simultaneously.
Key words: information security, information protection system, decision support system.

Стаття присвячена проблемі оцінки захисту інформаційної систем в реальних умовах експлуатації, що є однією з ключових задач підтримки необхідного рівня інформаційної безпеки в процесі життєвого циклу системи. Пропонується підхід до побудови системи підтримки прийняття рішення, що дозволяє за рахунок автоматизації процесу оцінки та використання накопиченого експертного досвіду одночасно підвищити якість оцінки і зменшити трудомісткість процесу оцінки.
Ключові слова: інформаційна безпека, система захисту інформації, система підтримки прийняття рішення.

Введение

Для любой информационной системы (ИС) важно не просто внедрить адекватные механизмы защиты, но и поддерживать требуемый уровень безопасности в процессе ее эксплуатации. Данная проблема находится в одном ряду с вопросами обеспечения отказоустойчивости ИТ-компонентов и работоспособности ИС в целом. Ее актуальность обусловлена неизбежностью эксплуатационных изменений ИС и среды (например, в результате обнаружения новых угроз или уязвимых мест, изменений требований пользователей, естественного развития и совершенствования системы и т.п.), вследствие которых возникает потребность:

– подтверждения того, что ранее установленные для ИС требования безопасности по-прежнему выполняются и обеспечивают необходимый уровень защищенности либо

– своевременного выявления необходимости модернизации системы защиты информации (СЗИ) в соответствии с произошедшими изменениями.

Цель данной работы – разработка методологического подхода к созданию системы поддержки принятия решений для автоматизации экспертной оценки уровня информационной безопасности ИС в реальных условиях эксплуатации.

Для достижения указанной цели необходимо было решить следующие **задачи**:

– дать общую характеристику типового процесса поддержки требуемого уровня информационной безопасности в виде цикла Дэминга и определить место в нем задачи оценки текущего уровня информационной безопасности;

– дать постановку задачи оценки текущего уровня информационной безопасности и определить показатели и критерии принятия решения;

– предложить и обосновать общий подход к решению задачи;

– предложить схему практической реализации подхода в виде системы поддержки принятия решения.

Общая характеристика задачи поддержки информационной безопасности

Процесс поддержки требуемого уровня информационной безопасности (ИБ) в ходе эксплуатации ИС разбивается на отдельные циклы. Один цикл представляет собой период от успешного завершения последней выполненной оценки ИС и начала эксплуатации разработанной/модернизированной системы до завершения следующей повторной оценки ИС.

Для реализации и поддержания информационной безопасности в ходе эксплуатации ИС целесообразно придерживаться циклической модели Деминга «... – планирование – реализация – проверка – совершенствование – планирование –...» в соответствии с СТБ ISO/IEC 27001-2011 [1].

Каждый из перечисленных на рис. 1 видов деятельности представляет самостоятельную задачу и может быть предметом отдельного исследования.

План по поддержке требуемого уровня ИБ идентифицирует основную линию поведения (мероприятия и процедуры) при изменениях ИС или среды. План специфичен для конкретной ИС и определяется в терминах категории компонентов, которые могут подвергнуться изменениям.

Решение задач, связанных с планированием возлагается на разработчика и независимого эксперта. В качестве нормативно-методической базы при ее решении можно использовать ISO/IEC 15408-3:2008, СТБ 34.101.3-2004 [2], [3].

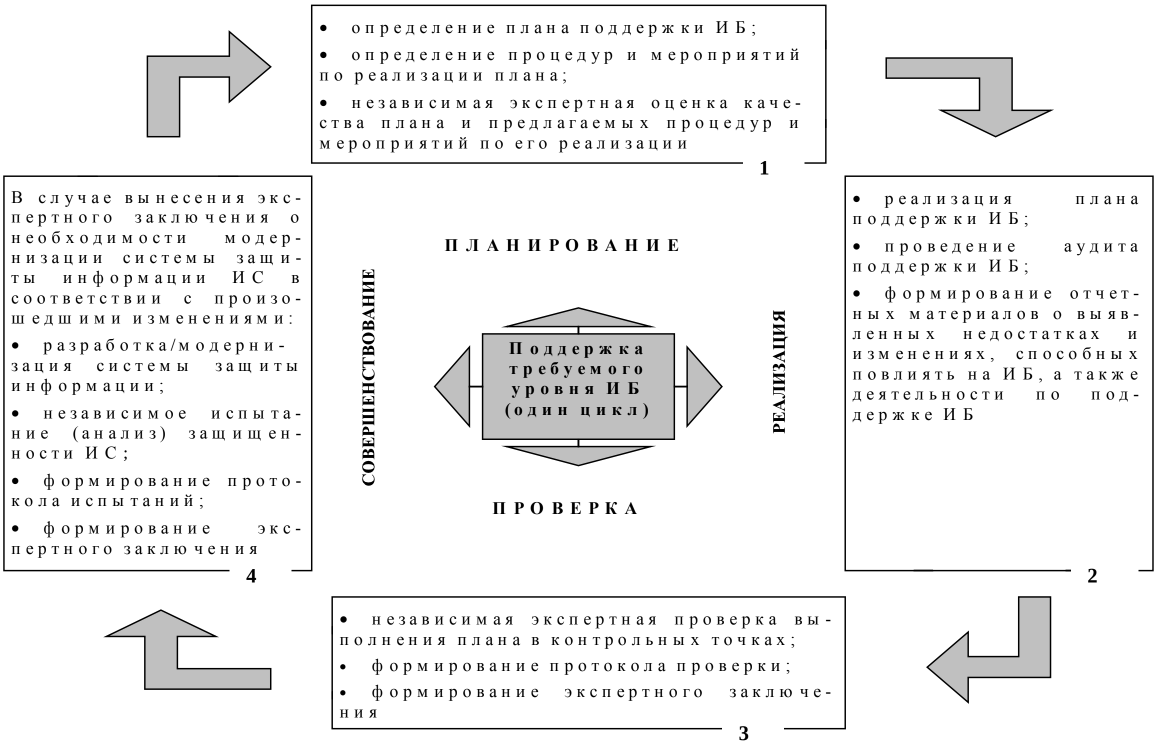


Рисунок 1 – Цикл Дэминга поддержки ИБ в процессе эксплуатации ИС

Реализация процесса поддержки ИБ в ходе эксплуатации ИС связана с решением целого ряда задач, включая:

– обеспечение мониторинга, регистрации и анализа изменений ИС или среды с точки зрения возможного их влияния на защищенность ИС;

– обеспечение мониторинга, регистрации, анализа и адекватной обработки выявляемых в ходе эксплуатации ИС недостатков и инцидентов безопасности;

– обеспечение необходимых текущих действий по поддержке требуемого уровня ИБ в ходе изменений ИС, включая обоснование корректности и достаточности предпринятых мер;

– обоснование того, что произошедшие изменения и выявленные недостатки находятся в пределах, установленных планом поддержки, вследствие чего требуемый уровень ИБ сохраняется и повторная оценка защищенности ИС не требуется.

Решение задач, связанных с реализацией процесса поддержки установленного уровня ИБ, возлагается на разработчика и организацию, эксплуатирующую ИС. В качестве нормативно-методической базы при ее решении можно использовать ISO/IEC 15408-3:2008, СТБ 34.101.3-2004, ISO/IEC 27002:2005, ISO/IEC 18045:2008 [2-5].

Независимая экспертная проверка состоит в периодическом контроле корректности действий разработчика. Цель проверки:

– подтвердить, что текущая версия ИС находится в пределах, установленных планом и повторная оценка защищенности ИС не требуется либо

– своевременно выявить потребность в модернизации СЗИ и проведении повторного испытания защищенности ИС.

В качестве нормативно-методической базы при проведении экспертной проверки можно использовать ISO/IEC 15408-3:2008, СТБ 34.101.3-2004, ISO/IEC 27002:2005, ISO/IEC 18045:2008 [2-5].

Проблема разработки/модернизации СЗИ решается в соответствии со сложившейся практикой разработки программных/программно-аппаратных средств.

Анализ и оценка защищенности ИС проводится путем обследования ИС в реальных условиях эксплуатации и возлагается на экспертов. Это сложный наукоемкий процесс, требующий знания исследуемой ИС, ее уязвимых мест, прогнозирования

угроз безопасности и порождаемых ими проблем информационной безопасности. В качестве нормативно-методической базы при проведении экспертной оценки можно использовать СТБ 34.101.3-2004, ISO/IEC 18045:2008 и Положение о порядке аттестации СЗИ, утвержденное постановлением Совета министров РБ № 675 [3-6]. Именно эта задача и является предметом рассмотрения данной статьи. Актуальность данной задачи обусловлена, с одной стороны, практической потребностью в получении адекватной и конструктивной оценки уровня защищенности ИС, а с другой стороны, отсутствием общепризнанных эффективных методик оценки, охватывающих весь спектр аспектов ИБ, влияющих на уровень защищенности ИС.

Постановка задачи

Задача оценки текущего состояния информационной безопасности ИС в процессе ее эксплуатации состоит в следующем.

Пусть S – некоторая функционирующая ИС, D – совокупность исходных данных и документов об ИС S, регламентированная в приложении 2 к Положению о порядке аттестации СЗИ из [6], и E – эксперт, на которого возложена оценка защищенности S. Требуется разработать комплексную методику экспертного обследования ИС, позволяющая оценить как отдельные аспекты безопасности ИС, так и информационную безопасность ИС в целом.

Пакет D исходных данных и документов представляется заявителем (разработчиком, организацией, эксплуатирующей ИС) и включает описание состава и структуры ИС, ее информационных потоков, перечень подлежащей защите обрабатываемой информации, модель потенциального нарушителя, описание системы защиты информации, правил разграничения доступа, организационной структуры ИС, технических средств и программного обеспечения, предназначенного для обработки защищаемой информации, средств физической защиты ИС, а также оцененное задание по безопасности и проектную, приемочную, эксплуатационную, организационно-распорядительную документацию, связанную с обеспечением ИБ.

Предполагается, что до инициирования процесса оценки ИС эксперт должен предварительно:

– оценить пригодность представленного пакета D. Возможный подход к проведению такой оценки, основанный на использовании показателей полноты, адекватности отображения и достаточности уровня детализации, предложен в [7];

– по согласованию с заявителем ознакомиться в целом с ИС и СЗИ непосредственно на территории расположения ИС. Эксперт заслушивает заявителя по общим вопросам, связанным с ИС и обеспечением ИБ (например, назначение, структура ИС, используемые аппаратные устройства, базовое программное обеспечение, функциональные возможности ИС, критичность обрабатываемой информации, узкие места ИС, ограничения на использование ИС, соответствие ИС стандартам, нормативным документам, требованиям политики безопасности, состав и структура СЗИ, порядок использования антивирусных средств, организационные мероприятия в области защиты информации, наличие и порядок использования эксплуатационной документации, включая руководства пользователей, эксплуатационные и должностные инструкции и т.п.) Заявитель демонстрирует работоспособность ИС и СЗИ и дает эксперту необходимые разъяснения.

Общая схема подхода

Оценка информационной безопасности ИС осуществляется путем обследования ИС в реальных условиях эксплуатации (на территории размещения ИС).

В рамках предлагаемой комплексной методики выделены следующие виды экспертной деятельности:

– обследование архитектуры ИС с целью проверки правильности ее отнесения к классу типовых объектов информатизации;

– обследование организационной структуры ИС, включая проверку уровня подготовки кадров и распределения ответственности персонала за организацию и обеспечение выполнения требований по защите информации;

– обследование состава и структуры комплекса технических средств и программного обеспечения. Проверка правильности выбора средств защиты информации;

– обследование технологического процесса обработки и хранения защищаемой информации и информационных потоков;

– обследование порядка применения программно-технических средств обработки информации и средств защиты информации;

– обследования порядка выполнения организационно-технических требований обеспечения информационной безопасности ИС на различных этапах жизненного цикла;

– проверка качества реализации функциональных требований безопасности к ИС и ИТ-среде ее эксплуатации (в соответствии с заданием по безопасности);

– оформление протокола оценки по результатам проведенного обследования, включающего формирование экспертного заключения об уровне информационной безопасности на текущем этапе эксплуатации ИС.

По каждому типу обследований определены:

– общие сведения о предмете обследования с позиций информационной безопасности;

– показатели, характеризующие с позиций ИБ качество реализации существенных для безопасности составляющих объекта обследования и

– совокупность проверок (единиц работы), которые рекомендуется выполнить эксперту по каждому из показателей качества, и руководящие указания по выполнению каждой единицы работы.

По результатам выполнения каждой единицы работы эксперт выставляет лингвистическую и уточняющую ее количественную оценку качества выполнения проверяемого свойства.

Для формирования экспертных оценок определена таблица соответствия, которая каждому допустимому лингвистической значению оценки сопоставляет числовой интервал значений.

Таблица 1 – Пример соответствия между лингвистической и интервальной шкалами оценок

Лингвистическая оценка степени соответствия	Интервал количественных оценок
Высокая степень соответствия	0,8 – 1,0
Средняя степень соответствия	0,6 – 0,79
Низкая степень соответствия	0,35 – 0,59
Несоответствие	0,01 – 0,34

Для каждой конкретной обследуемой ИС интервалы количественных оценок, указанные в табл. 1, подлежат корректировке, исходя из анализа существующих рисков безопасности.

Общая количественная оценка A^{ki} по показателю i, определенному в рамках обследования k, вычисляется на основании взвешенной аддитивной свертки оценок,

выставленных экспертом по результатам выполнения единиц работ, установленных для показателя *i* с учетом значимости каждой из проведенных проверок.

$$A^{ki} = \frac{\sum_{j=1}^{n_i} p_{kij} A^{kij}}{n_i},$$

где A^{kij} – количественная экспертная оценка по результатам выполнения проверки (единицы работы) j, p_{kij} – устанавливаемые экспертом веса, отражающие степень важности проверки j, n_i – количество единиц работы, выполняемых в рамках оценки по показателю i.

Общая количественная оценка A^k по результатам обследования k вычисляется на основании взвешенной аддитивной свертки оценок по совокупности показателей, оцениваемых в рамках обследования k с учетом значимости каждого из показателей

$$A^{k} = \frac{\sum_{i=1}^{t_k} p_{ki} A^{ki}}{t_k},$$

где p_{ki} – устанавливаемые экспертом веса, отражающие степень важности показателя i, t_k – количество показателей для обследования k.

Общая количественная оценка Δ^S информационной безопасности системы S на текущем этапе эксплуатации вычисляется как среднее арифметическое количественных оценок по результатам всех проведенных видов обследования

$$\Delta^{S} = \frac{\sum_{k=1}^{T_S} A^{k}}{T_S},$$

где T_S – количество проведенных видов обследования в ходе анализа системы S.

Лингвистические оценки по результатам отдельных обследований k и итоговая лингвистическая оценка текущей информационной безопасности системы S определяются на основании количественных оценок A^k и Δ^S соответственно по таблице 1.

Экспертное заключение формируется по каждому виду обследования с использованием следующего правила принятия решения.

1. С учетом анализа риска нарушения безопасности обследуемой ИС эксперт устанавливает нижний порог положительной лингвистической оценки результатов обследования.

2. Если в процессе экспертного обследования установлено, что оценка степени соответствия превышает установленный нижний порог лингвистической оценки или равна ему, то результат обследования считается положительным. В противном случае требуется доработка в части конкретного показателя.

3. Решение о предмете доработки принимается на согласительном совещании заявителя и исполнителя. При этом принимается одно из следующих решений:

– осуществить доработку СЗИ ИС или документа в течение установленного периода времени и провести повторную оценку в части проверки устранения выявленных недостатков;

– отказать в выдаче положительного заключения (в случае отказа заявителя от доработки).

Показатели и единицы работы

Показатели, единицы работы и рекомендации по их выполнению составляют методическое обеспечение для поддержки экспертного анализа ИБ ИС.

4.1 Для проверки правильности отнесения ИС к классу типовых объектов информатизации следует использовать стандарт СТБ 34.101.30-2007 [8], в котором устанавливается классификация объектов информатизации по требованиям обеспечения защиты обрабатываемой информации.

4.2 При обследовании организационной структуры ИС в качестве показателя оценки результатов обследования принята степень соответствия реальной организационной структуры организационной структуре, представленной в техническом проекте и в задании по безопасности. В состав экспертных проверок рекомендуется включить, например, следующие единицы работы:

– проверить качество документов, описывающих организационную структуру (документ, описывающий организационную структуру, должен содержать следующие разделы: изменения в организационной структуре управления объектом, организация подразделений, реорганизация существующих подразделений управления);

– выявить субъекты, влияющие на состояние ИБ ИС. Проверить, что к обеспечению ИБ привлекаются все влияющие на нее сотрудники, включая лиц участвующих в процессах автоматизированной обработки информации и технический персонал, обслуживающий ИС.

– проверить, соответствует ли реальная общая организационная структура ИС, а также реальная организационная структура СЗИ описаниям, приведенным в документации по техническому проектированию и задании по безопасности.

– проверить наличие категорирования ресурсов ИС в соответствии с проектной документацией и заданием по безопасности;

– проверить, соответствует ли реальное наличие структурных подразделений объекта информатизации перечню структурных подразделений, приведенному в проектной документации и задании по безопасности;

– проверить распределение функций, влияющих на обеспечение ИБ, между подразделениями в соответствии с проектной документацией и заданием по безопасности;

– проверить качество работы структурных подразделений в соответствии с проектной документацией и заданием по безопасности;

– проверить наличие и качество реализации взаимодействий между подразделениями и должностными лицами организации, способными повлиять на обеспечение ИБ;

– проверить наличие и качество текущего контроля за работой подразделений, изменениями в составе, структуре, решаемых задачах и подходах к решению данных задач, а также наличие текущей отчетности о работе подразделений и текущих изменениях перед вышестоящим руководством, подразделениями и должностными лицами, на работу которых могут повлиять произведенные изменения;

проверить наличие и качество выполнения процедур подготовки, принятия и реализации решений для руководителей и специалистов, управляющих информационной безопасностью ИС. Проверить наличие документально подтвержденного соответствия квалификации каждого сотрудника занимаемой им должности;

– проверить наличие необходимой квалификации и инструкций по безопасной эксплуатации ИС для разных категорий пользователей, влияющих на состояние информационной безопасности ИС. Проверить наличие регламентации действий пользователей и обслуживающего персонала ИС. Проверить наличие полного пакета инструкций, необходимых для безопасной эксплуатации ИС.

4.3 При обследовании состава и структуры комплекса технических средств и программного обеспечения обработки информации и защиты информации в качестве показателя оценки результатов обследования принята степень его соответствия проектной и эксплуатационной документации, техническому заданию на разработку ИС и заданию по безопасности.

4.4 При обследовании технологического процесса обработки и хранения защищаемой информации ИС в качестве показателя оценки результатов обследования принята степень успешности реализации операций технологического процесса.

Экспертная проверка должна охватывать вопросы общей организации технологического процесса (ТП), базовые операции сбора и регистрации данных, обработки данных, накопления и хранения данных, контроля и выдачи выходных данных, транспортирования (передачи и приема) данных, а также вопросы контроля за использованием ресурсов и обеспечения надежного уничтожения информации. В качестве рекомендуемых единиц работы, например, в части общей организации ТП можно указать следующие:

– проверить, соответствует ли предоставленное в документации описание ТП реальному обследуемому ТП;

– проверить, соответствуют ли объекты и субъекты доступа, идентифицированные в документации на ТП, реальным объектам и субъектам доступа ТП;

– проверить наличие документации по эксплуатации и обслуживанию ТП. Оценить качество информационного обеспечения ТП с точки зрения поддержки информационной безопасности;

– оценить надежность технического обеспечения ТП, используя для этого предоставленные заказчиком документы. Оценить достаточность уровня стандартизации и унификации составляющих компонентов ТП. Проверить степень сертифицированности используемых средств и оборудования;

– проверить, соответствует ли сложившаяся практика планирования и управления технологическим процессом предоставленной документации на ТП;

– проверить, соответствует ли структура и состав реализованной автоматизированной системы управления (АСУ) ТП описанию структуры и состава АСУ ТП, приведенному в документации. Проверить, обеспечивает ли реализованная АСУ ТП решение поставленных перед нею задач. Проверить удовлетворяет ли АСУ ТП критериям и требованиям, установленным для нее в документации на ТП. Проверить соответствует ли реальное техническое, программное, информационное обеспечение АСУ ТП описанию, приведенному в документации;

– проверить для каждой операции ТП наличие: названия, порядкового номера операции и номер предыдущей операции, указания того, является ли операция обязательной или опциональной, указания функционального назначения;

– проанализировать общую схему ТП с точки зрения выявления существующих возможностей доступа к обрабатываемой и передаваемой информации;

– проверить, соответствуют ли реализованные в ТП механизмы управления доступом инструкциям пользователя и администратора;

– проверить, предусмотрены ли в ТП механизмы сохранности активов при сбоях в работе и нарушении электропитания;

– проверить наличие средств контроля и борьбы со старением и преждевременным износом носителей данных, аппаратных средств, как средств предотвращения сбоев и отказов;

– проверить наличие средств контроля и предотвращения нарушений в работе аппаратных средств из-за неправильного использования или повреждения, в том числе из-за неправильного использования программных средств;

– проверить наличие специальных средств защиты от нарушений работоспособности компьютерных систем. В качестве специальных средств могут выступать: внесение структурной, временной, информационной и функциональной избыточности компьютерных ресурсов; защита от некорректного использования ресурсов компьютерной системы; выявление и своевременное устранение ошибок на этапах разработки программно-аппаратных средств;

– проверить соответствие используемых в ТП криптографических средств защиты национальным стандартам;

– оценить простоту и удобство использования средств администрирования;

– оценить, соответствует ли скорость обработки информации и время предоставления доступа к данным характеристикам, приведенным в документации;

– оценить регулярность и требуемую полноту тестирования целостности данных и программного обеспечения ТП;

– оценить качество резервного копирования критических данных и программного обеспечения ТП;

– оценить ТП по эргономическим показателям, способным повлиять на безопасность эксплуатации ТП;

– оценить приемлемость реальных затрат на обеспечение информационной безопасности ТП в соответствии с требованиями Технического задания и проектной документации;

– оценить степень соответствия выбранных значений регулируемых параметров ТП значениям нерегулируемых параметров ТП.

4.5 При обследовании информационных потоков в качестве показателя оценки используется надежность реализации информационных потоков как внутри ИС, так и между ИС и внешней средой. Используется следующий критерий принятия решений: реализация информационных потоков в полной мере соответствует требованиям, установленным в техническом задании, задании по безопасности, схемах обработки и передачи информации внутри ИС, а также между ИС и внешней средой, инструкции по обеспечению защиты информации ИС.

4.6 При обследовании порядка применения программно-технических средств обработки информации и средств защиты информации в качестве показателя оценки правильности применения средств обработки и защиты информации в ИС принято соответствие реализуемых процессов требованиям инструкций и других нормативных и организационно-распорядительных документов. Используется следующий критерий принятия решений: порядок применения программно-технических средств обработки информации и средств защиты информации в полной мере соответствует требованиям инструкции о порядке применения средств защиты информации ИС, инструкциям пользователя и администратора, схеме обработки и передачи данных (документов) в ИС, эксплуатационной документации, заданию по безопасности. В ходе данного обследования должны быть оценены: порядок допуска и регистрации пользователей; порядок оформления для пользователей ИС разрешения на передачу информации; порядок применения средств защиты информации в зависимости от требований по целостности, конфиденциальности и доступности обрабатываемой и передаваемой информации; реализация правил разграничения доступа, порядок использования средств антивирусной защиты при входе и проведении сеансов связи в ИС; порядок контроля за выполнением мероприятий по обеспечению информационной безопасности при эксплуатации ИС и др.

4.7 При обследовании порядка выполнения организационно-технических требований обеспечения информационной безопасности ИС в качестве показателя оценки реализации требований принята степень выполнения требований организационно-технического уровня. Используется следующий критерий принятия решений: реализация организационно-технических требований (порядок и процедуры обращения с защищаемой информацией, порядок применения СЗИ, в том числе уровень подготовки кадров и распределение ответственности за организацию и обеспечение защиты информации и т.д.) в полной мере соответствует заданию по безопасности, инструкциям пользователя и администратора.

4.8 При обследовании качества реализации функциональных требований безопасности в качестве показателя оценки используется степень реализации функциональных требований безопасности, сформулированных в задании по безопасности. Необходимо убедиться в выполнении требований безопасности к среде, предъявляемых в задании по безопасности и способных повлиять на безопасность функционирования ТП. Решение по данному виду обследования принимается на основе проведения тестирования ИС и сравнения степени совпадения фактических и ожидаемых результатов.

Практическая реализация подхода

Предлагаемый подход реализован в виде системы поддержки принятия решения, позволяющий автоматизировать процесс экспертного анализа. Разработанное методическое обеспечение представлено в виде баз знаний, содержащих перечень единиц работы и рекомендации по их выполнению. Эксперт в диалоговом режиме выставляет лингвистическую и количественную оценку по результатам выполнения каждой единицы работы из базы знаний. Вычисление обобщенных количественных и лингвистических оценок, а также формирование протокола анализа выполняется в автоматическом режиме. Общая схема работы системы поддержки принятия решения приведена на рис. 2.

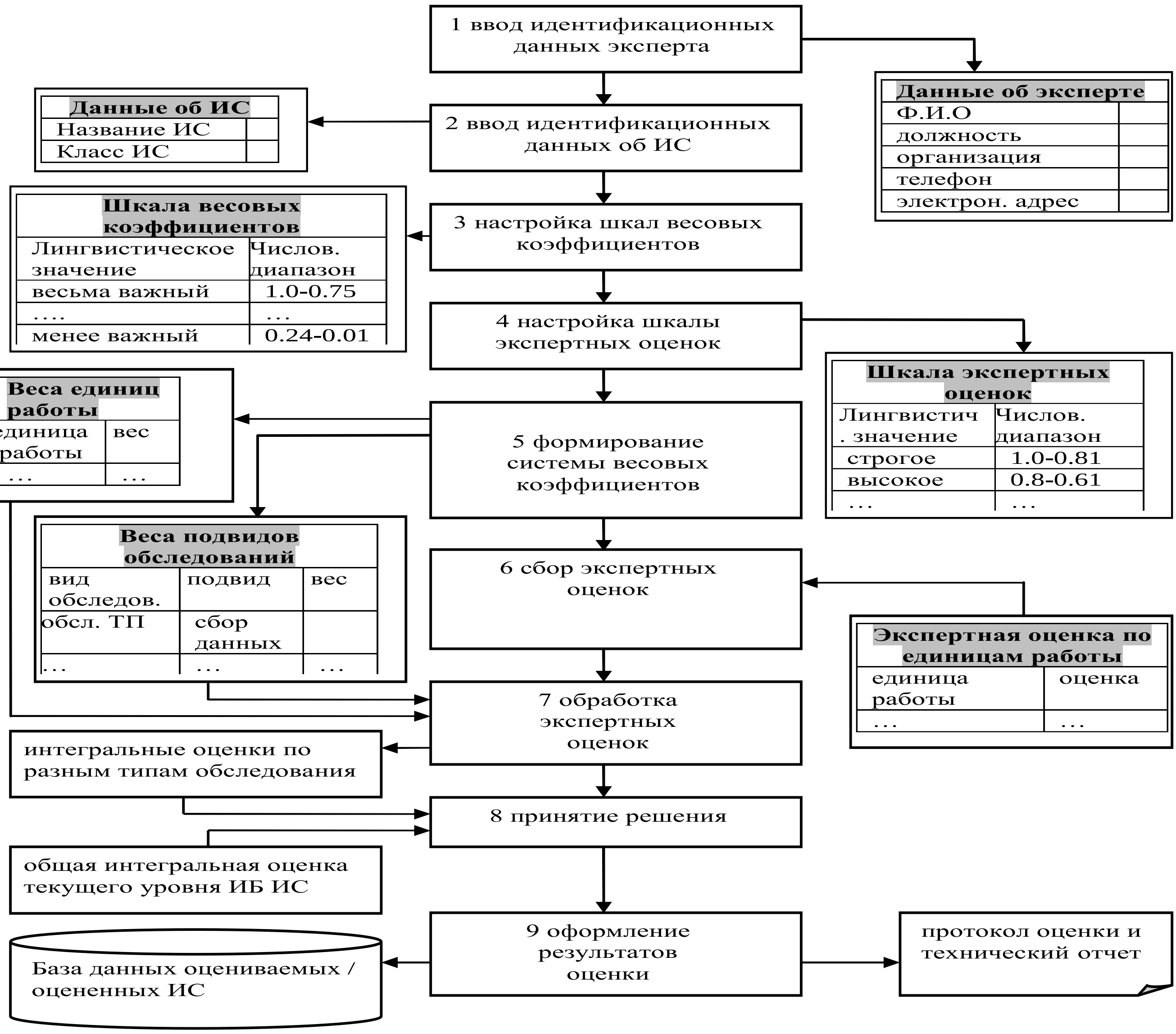


Рисунок 2 – Организационно-функциональная схема процедуры проведения экспертом анализа ИБ ИС

Заключение

Предложенная методика оценки безопасности ОИТ и основанная на ней автоматизированная система поддержки принятия решения позволит:

– гарантировать соответствие процесса оценки действующим стандартам;
– значительно снизить трудоемкость процесса оценки;
– получить более точные оценки;
– повысить обоснованность результата оценки.

Литература

1. СТБ ISO/IEC 27001-2011. Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
2. ISO/IEC 15408-3:2008. Information technology. Security techniques – Evaluation criteria for IT security-Part 3/ Security assurance components.
3. СТБ 34.101.3-2004 (ISO/IEC 15408-3:1999). Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3: Гарантийные требования безопасности.
4. ISO/IEC 27002:2005 ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for information security management.
5. ISO/IEC 18045:2008. Information technology – Security techniques – Methodology for IT security evaluation.
6. Постановление совета министров Республики Беларусь от 26 мая 2009 г. № 675 О некоторых вопросах защиты информации.
7. Максимович Е.П. Методологические основы разработки и применения показателей и критериев принятия решений при оценке документов в области информационной безопасности / Е.П. Максимович, В.К. Фисенко // Комплексная защита информации. Безопасность информационных технологий : материалы XVII межд. конф., 15 – 18 мая, Суздаль (Россия). – 2012. – С. 182-184.
8. СТБ 34.101.30-2007. Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация.

Literatura

1. STB ISO/IEC 27001-2011. Informacionnye tehnologii. Metody obespechenija bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Trebovanija.
2. ISO/IEC 15408-3:2008. Information technology. Security techniques – Evaluation criteria for IT security-Part 3/ Security assurance components.
3. STB 34.101.3-2004 (ISO/IEC 15408-3:1999). Informacionnye tehnologii i bezopasnost’. Kriterii ocenki bezopasnosti informacionnyh tehnologij. Chast’ 3: Garantijnye trebovanija bezopasnosti.
4. ISO/IEC 27002:2005 ISO/IEC 27002:2005. “Information technology - Security techniques - Code of practice for information security management”.
5. ISO/IEC 18045:2008. “Information technology - Security techniques - Methodology for IT security evaluation”.
6. Postanovlenie soveta ministrov Respubliki Belarus' ot 26 maja 2009 g. № 675 O nekotoryh voprosah zashhity informacii.
7. Maksimovich E.P., Kompleksnaja zashhita informacii. Bezopasnost’ informacionnyh tehnologij - materialy XVII mezhd. konf. 15-18 maja. Suzdal’ (Rossija). 2012 S. 182-184.
8. STB 34.101.30-2007 Informacionnye tehnologii. Metody i sredstva bezopasnosti. Ob’ekty informatizacii. Klassifikacija

REZUME

E.P. Maksimovich, A.B. Stepanyan, V.K. Fisenko

Methodological Foundations to Decision Support in the Analysis of Information Security during the Information System Operation

The paper deals with the problem of information systems security estimation in real-world conditions, as one of the key tasks of supporting the required level of information security during the life cycle of the system. The general characteristic of an information

security support problem, which general decision scheme is put in model of Deming Cycle "planning – realization – check – improvement", is given. The brief description of tasks arising within this scheme is given. The general statement of the information security current state estimation problem and the general scheme of the approach to its decision are given.

The expert analysis process is reduced to carrying out a number of inspections (architecture of information system, organizational structure of information system, composition and structure of a set of technical tools and software, technological process of processing and storage of protected information, information streams, an order of performance of organizational technical security requirements, quality check of realization of functional security requirements in real-world functioning conditions of information system). For each type of inspections, the estimation methodology containing the description of the set of recommended expert checks (work units) and the instruction on their performance is offered. By results of performance of each unit of work, the expert puts down a linguistic and specifying quantitative estimation. Integrated estimations on each type of inspection and the general integrated estimation of information system current information security are calculated, as the weighed additive parcels, on the basis of these estimations.

The approach is realized as a decision support system, allowing both to reduce costs and improve the quality of estimations.

Статья поступила в редакцию 01.06.2012.